SYS.1.1.A9 Einsatz von Virenschutz-Programmen auf Servern (B)

Abhängig vom installierten Betriebssystem, den bereitgestellten Diensten und von anderen vorhandenen Schutzmechanismen des Servers MUSS geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen und können. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein Virenschutz notwendig ist, aus den betreffenden Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums berücksichtigt werden.

SYS.1.1.A10 Protokollierung (B)

Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden, dazu gehören mindestens:

- Systemstarts und Reboots,
- erfolgreiche und erfolglose Anmeldungen am IT-System (Betriebssystem und Anwendungssoftware),
- fehlgeschlagene Berechtigungsprüfungen,
- blockierte Datenströme (Verstöße gegen ACLs oder Firewallregeln),
- Einrichtung oder Änderungen von Benutzenden, Gruppen und Berechtigungen,
- sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen) sowie
- Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Administrierenden und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.1.A12 Planung des Server-Einsatzes (S)

Jedes Server-System SOLLTE geeignet geplant werden. Dabei SOLLTEN mindestens folgende Punkte berücksichtigt werden:

- Auswahl der Plattform (Hardware oder virtualisierte Ressourcen), des Betriebssystems und der Anwendungssoftware,
- Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.),
- Art und Anzahl der Kommunikationsschnittstellen,
- Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform,
- administrative Zugänge (siehe SYS.1.1.A5 *Schutz von Schnittstellen*),
- Zugriffe von Benutzenden,
- Protokollierung (siehe SYS.1.1.A10 *Protokollierung*),
- Aktualisierung von Betriebssystem und Anwendungen sowie
- Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.1.1.A13 Beschaffung von Servern (S)

Bevor ein oder mehrere Server beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden.

SYS.1.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A15 Unterbrechungsfreie und stabile Stromversorgung (S) [Haustechnik]

Jeder Server SOLLTE an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden.

SYS.1.1.A16 Sichere Installation und Grundkonfiguration von Servern (S)

Der vollständige Installations- und Konfigurationsvorgang SOLLTE soweit wie möglich innerhalb einer gesonderten und von Produktivsystemen abgetrennten Installationsumgebung vorgenommen werden. Die Konfiguration des Betriebssystems SOLLTE vor produktiver Inbetriebnahme des Servers bereits vorgenommen sein.

Mehrere wesentliche Funktionen und Rollen SOLLTEN NICHT durch einen einzigen Server erfüllt, sondern geeignet aufgeteilt werden.

Alle sicherheitsrelevanten Einstellungen der aktivierten Dienste und Funktionen (vgl. SYS.1.1.A6 *Deaktivierung nicht benötigter Dienste*) SOLLTEN entsprechend den Vorgaben der Sicherheitsrichtlinie für Server (siehe SYS.1.1.A11 *Festlegung einer Sicherheitsrichtlinie für Server)* konfiguriert, getestet und regelmäßig inhaltlich überprüft werden. Dabei SOLLTE der Server unter Berücksichtigung der Empfehlungen des Betriebssystemherstellers und des voreingestellten Standardverhaltens konfiguriert werden, sofern dies nicht anderen Anforderungen aus dem IT-Grundschutz oder der Organisation widerspricht. Die Entscheidungen SOLLTEN dokumentiert und begründet werden. Konfigurationsoptionen SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn das voreingestellte Standardverhalten dadurch nicht verändert wird.

Sofern der Server eine Verbindung in das Internet benötigt oder aus dem Internet erreichbar sein muss, SOLLTE er erst mit dem Internet verbunden werden, nachdem die Installation und die Konfiguration abgeschlossen sind.

SYS.1.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A19 Einrichtung lokaler Paketfilter (S)

Vorhandene lokale Paketfilter SOLLTEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle sowie Ports und Schnittstellen beschränkt wird. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.

SYS.1.1.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A21 Betriebsdokumentation für Server (S)

Betriebliche Aufgaben, die an einem Server durchgeführt werden, SOLLTEN nachvollziehbar dokumentiert werden (Wer?, Wann?, Was?). Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Sicherheitsrelevante Aufgaben, z. B. wer befugt ist, neue Festplatten einzubauen, SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE gegen unbefugten Zugriff und Verlust geschützt werden.

SYS.1.1.A22 Einbindung in die Notfallplanung (S)

Der Server SOLLTE im Notfallmanagementprozess berücksichtigt werden. Dazu SOLLTEN die Notfallanforderungen an den Server ermittelt und geeignete Notfallmaßnahmen umgesetzt werden, z. B. indem Wiederanlaufpläne erstellt oder Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

SYS.1.1.A23 Systemüberwachung und Monitoring von Servern (S)

Das Server-System SOLLTE in ein geeignetes Systemüberwachungs- oder Monitoringkonzept eingebunden werden. Der Systemzustand sowie die Funktionsfähigkeit des Servers und der darauf betriebenen Dienste SOLLTEN laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN an das Betriebspersonal gemeldet werden.

SYS.1.1.A24 Sicherheitsprüfungen für Server (S)

Server SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die überprüfen, ob alle Sicherheitsvorgaben eingehalten werden und gegebenenfalls vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen SOLLTEN insbesondere auf Servern mit externen Schnittstellen durchgeführt werden. Um mittelbare Angriffe über infizierte IT-Systeme im eigenen Netz zu vermeiden, SOLLTEN jedoch auch interne Server in festgelegten Zyklen entsprechend überprüft werden. Es SOLLTE geprüft werden, ob die Sicherheitsprüfungen automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers (S)

Bei der Außerbetriebnahme eines Servers SOLLTE sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf dem Server gespeichert sind. Es SOLLTE rechtzeitig sichergestellt werden, dass vom Server angebotene Dienste durch einen anderen Server übernommen werden, wenn dies erforderlich ist.

Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines Servers abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zu Datensicherung, Migration von Diensten und dem anschließenden sicheren Löschen aller Daten umfassen.

SYS.1.1.A35 Erstellung und Pflege eines Betriebshandbuchs (S)

Es SOLLTE ein Betriebshandbuch erstellt werden. Darin SOLLTEN alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Server zu betreiben. Für jede Art von Server SOLLTE es ein spezifisches Betriebshandbuch geben. Das Betriebshandbuch SOLLTE regelmäßig aktualisiert werden. Das Betriebshandbuch SOLLTE vor unberechtigtem Zugriff geschützt werden. Das Betriebshandbuch SOLLTE in Notfällen zur Verfügung stehen.

SYS.1.1.A37 Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (S)

Um sowohl den unberechtigten Zugriff auf das Betriebssystem oder andere Anwendungen bei Angriffen als auch den Zugriff vom Betriebssystem auf besonders schützenswerte Dateien zu verhindern, SOLLTEN Anwendungen und Betriebssystemkomponenten (wie beispielsweise Authentisierung oder Zertifikatsüberprüfung) ihrem Schutzbedarf entsprechend besonders gekapselt oder anderen Anwendungen und Betriebssystemkomponenten gegenüber isoliert werden. Dabei SOLLTEN insbesondere sicherheitskritische Anwendungen berücksichtigt werden, die mit Daten aus unsicheren Quellen arbeiten (z. B. Webbrowser und Bürokommunikations-Anwendungen).

SYS.1.1.A39 Zentrale Verwaltung der Sicherheitsrichtlinien von Servern (S)

Alle Einstellungen des Servers SOLLTEN durch Nutzung eines zentralen Managementsystems (siehe auch OPS.1.1.7 *Systemmanagement*) verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert sein. Technisch nicht umsetzbare Konfigurationsparameter SOLLTEN dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.1.A26 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A27 Hostbasierte Angriffserkennung (H)

Hostbasierte Angriffserkennungssysteme (Host-based Intrusion Detection Systems, IDS und Intrusion Prevention Systems, IPS) SOLLTEN eingesetzt werden, um das Systemverhalten auf Anomalien und Missbrauch hin zu überwachen. Die eingesetzten IDS/IPS-Mechanismen SOLLTEN geeignet ausgewählt, konfiguriert und ausführlich getestet werden. Bei einer Angriffserkennung SOLLTE das Betriebspersonal in geeigneter Weise alarmiert werden.

Über Betriebssystem-Mechanismen oder geeignete Zusatzprodukte SOLLTEN Veränderungen an Systemdateien und Konfigurationseinstellungen überprüft, eingeschränkt und gemeldet werden.

SYS.1.1.A28 Steigerung der Verfügbarkeit durch Redundanz (H)

Server mit hohen Verfügbarkeitsanforderungen SOLLTEN gegen Ausfälle in geeigneter Weise geschützt sein. Hierzu SOLLTEN mindestens geeignete Redundanzen verfügbar sein sowie Wartungsverträge mit den Lieferanten abgeschlossen werden. Es SOLLTE geprüft werden, ob bei sehr hohen Anforderungen Hochverfügbarkeitsarchitekturen mit automatischem Failover, gegebenenfalls über verschiedene Standorte hinweg, erforderlich sind.

SYS.1.1.A29 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A30 Ein Dienst pro Server (H)

Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste SOLLTE auf jedem Server jeweils nur ein Dienst betrieben werden.

SYS.1.1.A31 Einsatz von Ausführungskontrolle (H)

Es SOLLTE über eine Ausführungskontrolle sichergestellt werden, dass nur explizit erlaubte Programme und Skripte ausgeführt werden können. Die Regeln SOLLTEN so eng wie möglich gefasst werden. Falls Pfade und Hashes nicht explizit angegeben werden können, SOLLTEN alternativ auch zertifikatsbasierte oder Pfad-Regeln genutzt werden.

SYS.1.1.A32 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A33 Aktive Verwaltung der Wurzelzertifikate (H)

Im Zuge der Beschaffung und Installation des Servers SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Servers notwendig sind. Auf dem Server SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden.

SYS.1.1.A34 Festplattenverschlüsselung (H)

Bei erhöhtem Schutzbedarf SOLLTEN die Datenträger des Servers mit einem als sicher geltenden Produkt oder Verfahren verschlüsselt werden. Dies SOLLTE auch für virtuelle Maschinen mit produktiven Daten gelten. Es SOLLTE nicht nur ein TPM allein als Schlüsselschutz dienen. Das Wiederherstellungspasswort SOLLTE an einem geeigneten sicheren Ort gespeichert werden. Bei sehr hohen Anforderungen z. B. an die Vertraulichkeit SOLLTE eine Full Volume oder Full Disk Encryption erfolgen.

SYS.1.1.A36 Absicherung des Bootvorgangs (H)

Bootloader und Betriebssystem-Kern SOLLTEN durch selbstkontrolliertes Schlüsselmaterial signiert beim Systemstart in einer vertrauenswürdigen Kette geprüft werden (Secure Boot). Nicht benötigtes Schlüsselmaterial SOLLTE entfernt werden.

SYS.1.1.A38 Härtung des Host-Systems mittels Read-Only-Dateisystem (H)

Die Integrität des Host-Systems SOLLTE durch ein Read-Only-Dateisystem sichergestellt werden (Immutable OS).

4. Weiterführende Informationen

4.1. Wissenswertes

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Guide to General Server Security: NIST Special Publication 800-123“, Juli 2008 zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.2.2 Windows Server 2012

1. Beschreibung

1.1. Einleitung

Mit Windows Server 2012 hat Microsoft im September 2012 ein Betriebssystem für Server auf den Markt gebracht, das diverse Verbesserungen der Sicherheit gegenüber bisherigen Windows-Versionen, insbesondere auch gegenüber dem Vorgänger Windows Server 2008 R2, mitbringt. Technisch wird dabei nicht auf Windows Server 2008 R2 aufgebaut, sondern auf der Codebasis des Client-Betriebssystems Windows 8. Mit dem Release Windows Server 2012 R2 im Oktober 2013 wurde das Betriebssystem nochmals aktualisiert und erweitert, um es zum Server-Äquivalent zu Windows 8.1 auf der Clientseite zu machen.

Dieser Baustein beschäftigt sich mit der Absicherung von Windows Server 2012 und Windows Server 2012 R2 gleichermaßen. Wenn beide Versionen gemeint sind, wird die einheitliche Schreibweise „Windows Server 2012" verwendet. Unterschiede in der Version R2 werden gesondert erwähnt. Das Ablaufdatum für den Mainstream Support bzw. den Extended Support („End-of-Life", EOL) ist für beide Betriebssysteme der 09.10.2018 bzw. der 10.10.2023.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen und Prozessen, die durch Server-Systeme auf Basis von Windows Server 2012 im Regelbetrieb verarbeitet bzw. gesteuert werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.2.2 *Windows Server 2012* ist für alle Server-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows Server 2012 eingesetzt wird. Für neuere Versionen von Windows Server gibt es den Baustein SYS.1.2.3 *Windows Server*.

Dieser Baustein konkretisiert und ergänzt die Aspekte, die im Bausteinen SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Windows Server 2012. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

Im Rahmen dieses Bausteins wird von einer Standardeinbindung in eine Active-Directory-Domäne ausgegangen, wie sie in Institutionen üblich ist. Besonderheiten von Stand-alone-Systemen werden nur punktuell dort erwähnt, wo die Unterschiede besonders relevant erscheinen. Anforderungen zum Thema Active Directory sind Bestandteil des Bausteins APP.2.2 *Active Directory Domain Services*.

Sicherheitsanforderungen möglicher Serverrollen und -funktionen wie Fileserver (APP.3.3 *Fileserver*), Webserver (APP.3.2 *Webserver*) oder Microsoft Exchange und Outlook (APP.5.2 *Microsoft Exchange und Outlook*) sind Gegenstand eigener Bausteine, genauso wie das Thema Virtualisierung (SYS.1.5 *Virtualisierung*). In diesem Baustein geht es um die grundlegende Absicherung auf Betriebssystemebene mit bordeigenen Mitteln, unabhängig vom Einsatzzweck des Servers.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.2.2 *Windows Server 2012* von besonderer Bedeutung.

2.1. Unzureichende Planung von Windows Server 2012

Windows Server 2012 ist ein komplexes Betriebssystem mit einer großen Anzahl an Funktionen und Konfigurationsoptionen. Bei der Einbindung in die Domäne und bei der Vernetzung mit anderen IT-Systemen und Diensten gibt es sehr viele Spielräume. Auch wenn moderne Windows-Versionen in vielen Bereichen gute Standardeinstellungen mitbringen, ist die Grundkonfiguration nicht in jedem Fall die sicherste. Dies kann bei unzureichender Planung zu einer Vielzahl von Angriffsvektoren führen, die von unberechtigten Dritten leicht ausgenutzt werden können. Werden außerdem nicht schon vor der Installation zentrale Entscheidungen getroffen, wird Windows Server 2012 in einem unsicheren und undefinierten Zustand ausgeführt, der sich nachträglich kaum mehr beheben lässt.

2.2. Unbedachte Cloud-Nutzung

Windows Server 2012 bietet an verschiedenen Stellen die Möglichkeit, Cloud-Dienste zu nutzen, ohne dass dafür Drittsoftware installiert werden muss. Hierzu gehören beispielsweise Microsoft Azure Online Backup oder die Online-Speicherung von BitLocker-Wiederherstellungsschlüsseln. Während Cloud-Dienste grundsätzlich Vorteile, beispielsweise hinsichtlich der Verfügbarkeit, bieten können, bestehen bei unbedachtem Einsatz Risiken für die Vertraulichkeit sowie eine zusätzliche Abhängigkeit. So können Daten über Cloud-Dienste in die Hände unberechtigter Personen gelangen. Dabei kann es sich sowohl um kriminell als auch um staatlich Agierende handeln. Wird ein Cloud-Dienst eingestellt, kann dies erhebliche Auswirkungen auf die eigenen Geschäftsprozesse haben.

2.3. Fehlerhafte Administration von Windows-Servern

Windows Server 2012 und Windows Server 2012 R2 haben im Vergleich zu den Vorgängerversionen viele neue sicherheitsrelevante Funktionen hinzubekommen. Bei anderen (bekannten) Features haben sich Teilfunktionen, Parameter oder Standardkonfigurationen verändert. Ist der IT-Betrieb nicht ausreichend in den Besonderheiten der Systeme geschult, drohen Konfigurationsfehler und menschliche Fehlhandlungen, die neben der Funktionalität auch die Sicherheit des Systems beeinträchtigen können.

Eine besondere Gefahr stellen uneinheitliche Windows-Server-Sicherheitseinstellungen dar (z. B. bei SMB, RPC oder LDAP). Wenn die Konfiguration nicht systematisch und zentral geplant, dokumentiert, überprüft und nachgehalten wird, droht ein sogenannter Konfigurationsdrift. Je mehr sich die konkreten Konfigurationen funktional ähnlicher Systeme unbegründet und undokumentiert auseinander bewegen, desto schwieriger wird es, einen Überblick über den Status quo zu behalten und die Sicherheit ganzheitlich und konsequent aufrechtzuerhalten.

2.4. Unsachgemäßer Einsatz von Gruppenrichtlinien (GPOs)

Gruppenrichtlinien (Group Policy Objects, GPOs) sind eine nützliche und mächtige Art, viele (Sicherheits-)Aspekte von Windows Server 2012 zu konfigurieren, insbesondere in einer Domäne. Bei der großen Zahl möglicher Einstellungen passiert es leicht, versehentlich widersprüchliche oder inkompatible Einstellungen zu setzen oder Themenbereiche zu vergessen. Dies führt bei unsystematischer Vorgehensweise mindestens zu Betriebsstörungen, die teilweise nur schwer zu beheben sind, und schlimmstenfalls zu schwerwiegenden Schwachstellen auf dem Server oder auf verbundenen Clients. Insbesondere falsch verstandene Vererbungsregeln und Filter können dazu führen, dass GPOs gar nicht auf ein System angewendet werden.

2.5. Integritätsverlust schützenswerter Informationen oder Prozesse

Windows Server 2012 verfügt über eine Vielzahl von Funktionen, um die Integrität von durch das Betriebssystem verarbeiteten Informationen zu schützen. Jede einzelne dieser Funktionen kann mit Schwachstellen behaftet sein. Zudem mangelt es häufig an einer konsequenten Konfiguration, nicht zuletzt aus Gründen der Bequemlichkeit. Informationen und Prozesse können so durch Unbefugte verfälscht und oftmals sogar die Spuren verwischt werden. Häufig werden auch Schadprogramme eingesetzt, um Informationen aus der Ferne zu manipulieren.

2.6. Unberechtigtes Erlangen oder Missbrauch von Administrationsrechten

Die reguläre Arbeit unter Standardberechtigungen ist inzwischen gängige Praxis. Da Administrierende jedoch an bestimmten Stellen trotzdem ihre Rechte erhöhen müssen, können Angreifende dort potenziell privilegierte Rechte erlangen. Auch ein Missbrauch von Rechten durch legitime Administrierende ist ein relevantes Schadensszenario. Da die Rollen oft sehr mächtig sind, sind hier die Auswirkungen in der Regel beträchtlich, insbesondere bei sogenannten Domänenadministratoren. Auch ohne Passwörter zu erraten oder zu brechen, können z. B. durch soge-

nannte Pass-the-Hash-Verfahren geeignete Credentials ausgelesen und missbraucht werden, um sich lateral im Netz weiterzubewegen.

2.7. Kompromittierung von Fernzugängen

Da Windows Server 2012 über eine Vielzahl von Möglichkeiten verfügt, aus der Ferne verwaltet zu werden, können diese grundsätzlich auch missbraucht werden. Fernzugänge wie z. B. RDP-Sitzungen können durch unsichere bzw. unsicher verwendete Protokolle, schwache Authentifizierung (z. B. schwache Passwörter) oder fehlerhafte Konfiguration für Dritte erreichbar sein. Hierdurch können der Server und die dort gespeicherten Informationen weitgehend kompromittiert werden. Oft können auf diese Weise auch weitere mit dem Server verbundene IT-Systeme kompromittiert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.2.2 *Windows Server 2012* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.2.2.A1 Planung von Windows Server 2012 (B)

Der Einsatz von Windows Server 2012 MUSS vor der Installation sorgfältig geplant werden. Die Anforderungen an die Hardware MÜSSEN vor der Beschaffung geprüft werden. Es MUSS eine begründete und dokumentierte Entscheidung für eine geeignete Edition des Windows Server 2012 getroffen werden. Der Einsatzzweck des Servers sowie die Einbindung ins Active Directory MÜSSEN dabei spezifiziert werden. Die Nutzung von ins Betriebssystem integrierten Cloud-Diensten MUSS grundsätzlich abgewogen und geplant werden. Wenn nicht benötigt, MUSS die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

SYS.1.2.2.A2 Sichere Installation von Windows Server 2012 (B)

Es DÜRFEN KEINE anderen als die benötigten Serverrollen und Features bzw. Funktionen installiert werden. Wenn es vom Funktionsumfang her ausreichend ist, MUSS die Server-Core-Variante installiert werden. Andernfalls MUSS begründet werden, warum die Server-Core-Variante nicht genügt. Der Server MUSS bereits während der Installation auf einen aktuellen Patch-Stand gebracht werden.

SYS.1.2.2.A3 Sichere Administration von Windows Server 2012 (B)

Alle Administrierenden, die für das Server-System zuständig sind, MÜSSEN in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 geschult sein. Webbrowser auf dem Server DÜRFEN NICHT zum Surfen im Web verwendet werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.2.2.A4 Sichere Konfiguration von Windows Server 2012 (S)

Mehrere wesentliche Funktionen bzw. Rollen SOLLTEN NICHT durch einen einzigen Server erfüllt, sondern geeignet aufgeteilt werden. Vor Inbetriebnahme SOLLTE das System grundlegend gehärtet werden. Dafür SOLLTEN funktionsspezifische und institutionsweite Sicherheitsvorlagen erstellt und gepflegt werden, die auf die Server ausgerollt werden. Der Internet Explorer SOLLTE auf dem Server nur in der Enhanced Security Configuration und im Enhanced Protected Mode genutzt werden.

SYS.1.2.2.A5 Schutz vor Schadsoftware auf Windows Server 2012 (S)

Außer bei IT-Systemen mit Windows Server 2012, die als Stand-alone-Gerät ohne Netzanschluss und Wechselmedien betrieben werden, SOLLTE vor dem ersten Verbinden mit dem Netz oder Wechselmedien ein Virenschutzprogramm installiert werden. Im Konzept zum Schutz vor Schadsoftware SOLLTE vorgesehen werden, dass regelmäßig alle Festplatten vollständig gescannt werden. Es SOLLTEN Alarme für Virenfunde konfiguriert sein.

SYS.1.2.2.A6 Sichere Authentisierung und Autorisierung in Windows Server 2012 (S)

In Windows Server 2012 R2 SOLLTEN alle Konten von Benutzenden Mitglied der Sicherheitsgruppe „Geschützte Nutzer" sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von „Geschützte Nutzer" sein. Dienste-Konten in Windows Server 2012 SOLLTEN Mitglied der Gruppe „Managed Service Account" sein. Der PPL-Schutz des Local Credential Store LSA SOLLTE aktiviert werden. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen SOLLTE bevorzugt werden.

SYS.1.2.2.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.2.2.A8 Schutz der Systemintegrität (S)

AppLocker SOLLTE aktiviert und möglichst strikt konfiguriert sein.

SYS.1.2.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.2.2.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.2.2.A11 Angriffserkennung bei Windows Server 2012 (H)

Sicherheitsrelevante Ereignisse in Windows Server 2012 SOLLTEN an einem zentralen Punkt gesammelt und ausgewertet werden. Verschlüsselte Partitionen SOLLTEN nach einer definierten Anzahl von Entschlüsselungsversuchen gesperrt werden.

SYS.1.2.2.A12 Redundanz und Hochverfügbarkeit bei Windows Server 2012 (H)

Es SOLLTE geprüft werden, welche Verfügbarkeitsanforderungen durch Betriebssystemfunktionen wie Distributed File System (DFS), ReFS, Failover Cluster und Network Load Balancing bzw. NIC-Teaming (LBFO) erfüllt oder unterstützt werden können. Für Außenstellen SOLLTE BranchCache aktiviert werden.

SYS.1.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.2.2.A14 Herunterfahren verschlüsselter Server und virtueller Maschinen (H)

Um verschlüsselte Daten zu schützen, SOLLTEN nicht benötigte Server (inklusive virtuelle Maschinen) immer heruntergefahren werden. Dies SOLLTE möglichst automatisiert erfolgen. Die Entschlüsselung der Daten SOLLTE einen interaktiven Schritt erfordern oder zumindest im Sicherheitsprotokoll festgehalten werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Der Hersteller Microsoft stellt unter anderem folgende weiterführende Informationen zu Windows Server 2012 bereit:

- Secure Windows (für Windows 8/8.1, gilt größtenteils auch für Windows Server 2012 / 2012 R2): https://technet.microsoft.com/en-us/library/hh832031.aspx
- Secure Windows Server 2012 R2 and Windows Server 2012: https://technet.microsoft.com/en-us/library/hh831360.aspx
- Security and Protection: https://technet.microsoft.com/en-us/library/hh831778.aspx
- Liste von Sicherheitsereignissen unter Windows 8.1 und Windows Server 2012: https://www.microsoft.com/en-us/download/confirmation.aspx?id=50034
- Konfigurieren von zusätzlichem LSA-Schutz: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- Windows Server Guidance to protect against Speculative Execution: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-speculative-execution

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security", insbesondere in Area SY1.2 Server Configuration, Vorgaben für den Einsatz von Servern.

Das National Institute of Standards and Technology (NIST) stellt das Dokument ,,Guide to General Server Security: NIST Special Publication 800-123", Juli 2008 zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.2.3 Windows Server

1. Beschreibung

1.1. Einleitung

Mit Windows Server bietet Microsoft ein Betriebssystem für Server an. Bei den Hauptversionen 2016, 2019 und 2022 von Windows Server handelt es sich um sogenannte Langzeit-Versionen (Long-Term Servicing Channel, LTSC), die jeweils auf der Codebasis des Client-Betriebssystems Windows 10 basieren. Wie bei Windows 10 liefert Microsoft auch mit Windows Server zunehmend cloudbasierte Funktionen und Anwendungen sowie Schnittstellen zur Microsoft Azure Cloud-Plattform mit aus.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen, die durch Server-Systeme auf Basis von Windows Server 2016, 2019 und 2022 im Regelbetrieb verarbeitet, gespeichert und darüber übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.2.3 *Windows Server* ist auf alle Server-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows Server in den Versionen 2016, 2019 oder 2022 eingesetzt wird. Für Windows Server 2012 ist stattdessen der Baustein SYS.1.2.2 *Windows Server 2012* zu modellieren.

Dieser Baustein konkretisiert und ergänzt die plattformunabhängigen Sicherheitsaspekte für Server, die im Bausteinen SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Windows Server in den genannten Versionen. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

In diesem Baustein geht es um die grundlegende Absicherung auf Betriebssystemebene mit bordeigenen Mitteln, unabhängig vom Einsatzzweck des Servers. Sicherheitsanforderungen möglicher Serverrollen und -funktionen wie beispielsweise Fileserver (APP.3.3 *Fileserver*) oder Webserver (APP.3.2 *Webserver*) sind Gegenstand eigener Bausteine, genauso wie das Thema Virtualisierung (SYS.1.5 *Virtualisierung*).

Darüber hinaus sind im Funktionsumfang einiger Betriebssystemvarianten auch weitere Anwendungen vorinstalliert, wie etwa der Microsoft Internet Explorer als Browser. Für diese Anwendungen sind die entsprechenden Bausteine zu modellieren.

Im Rahmen dieses Bausteins wird von einer Aufnahme als „Member Server“ in eine Active-Directory-Domäne ausgegangen, wie sie in Institutionen üblich ist. Besonderheiten von Stand-alone-Systemen werden nur punktuell dort erwähnt, wo die Unterschiede besonders relevant erscheinen. Anforderungen zum Thema Active Directory sind Bestandteil des Bausteins APP.2.2 *Active Directory Domain Services*. Für die Nutzung der teils mitgelieferten Funktionen und Anwendungen von Cloud-Diensten sowie Schnittstellen zwischen der Microsoft Azure Cloud-Plattform und Windows Server muss der Baustein OPS.2.2 *Cloud-Nutzung* angewendet werden, in dem auch Gefährdungen und generelle Anforderungen bei der Cloud-Nutzung behandelt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.2.3 *Windows Server* von besonderer Bedeutung.

2.1. Unbedachte Cloud-Nutzung

Windows Server bietet an verschiedenen Stellen die Möglichkeit, Cloud-Dienste zu nutzen, ohne dass dafür Drittsoftware installiert werden muss. Hierzu gehören beispielsweise Microsoft Azure Online Backup oder die Online-Speicherung von BitLocker-Wiederherstellungsschlüsseln. Während Cloud-Dienste mögliche Vorteile, beispielsweise hinsichtlich der Verfügbarkeit, bieten können, bestehen bei unbedachtem Einsatz beispielsweise Risiken für die Vertraulichkeit sowie eine Abhängigkeit von Dienstleistenden. So können Daten über Cloud-Dienste in die Hände unberechtigter Dritter gelangen. Dabei kann es sich sowohl um Kriminelle als auch um staatliche Akteure handeln. Wird ein Cloud-Dienst durch den Anbieter beendet, kann dies erhebliche Auswirkungen auf die eigenen Geschäftsprozesse haben.

2.2. Kompromittierung von Fernzugängen

Da Windows Server über eine Vielzahl von Möglichkeiten verfügt, aus der Ferne verwaltet zu werden, können diese grundsätzlich auch missbraucht werden. Fernzugänge wie z. B. RDP- oder WinRM-Ssitzungen können durch unsichere oder unsicher verwendete Protokolle, schwache Authentisierungsverfahren (z. B. schwache Passwörter) oder fehlerhafte Konfiguration für Dritte erreichbar sein. Hierdurch können der Server und die dort gespeicherten Informationen weitgehend kompromittiert werden. Oft können auf diese Weise auch weitere mit dem Server verbundene IT-Systeme kompromittiert werden.

2.3. Telemetrie von Windows Server

Windows Server sendet standardmäßig sogenannte Diagnosedaten an den Hersteller Microsoft. Zusätzlich kann Microsoft über den in Windows Server integrierten Telemetriedienst gezielt Informationen von einem Server abfragen. Abhängig vom Telemetrie-Level schließt dies beispielsweise den Zugriff auf Absturzabbilder des Speichers (sog. „Crash Dumps“) sowie den Zugriff auf Betriebssystemereignisse auf dem Server mit ein. Es besteht die Gefahr, dass die Diagnose- und Telemetriedaten schützenswerte Informationen enthalten, die auf diesem Weg an Dritte gelangen können.

2.4. Eingeschränkte Forensik bei der Nutzung des Virtual Secure Mode (VSM)

Durch die Nutzung des Virtual Secure Mode (VSM) werden forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt oder erschwert. Prozesse, die durch den Secure Kernel oder den Isolated User Mode (IUM) geschützt werden, sind nicht mehr zugänglich. Beispielsweise können Speicherabbilder dieser Prozesse aufgrund kryptografischer Maßnahmen nicht ausgewertet werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.2.3 *Windows Server* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.2.3.A1 Planung von Windows Server (B)

Es MUSS eine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server getroffen werden. Der Einsatzzweck des Servers sowie die Einbindung ins Active Directory MÜSSEN dabei spezifiziert werden. Die Nutzung von mitgelieferten Cloud-Diensten im Betriebssystem MUSS grundsätzlich abgewogen und gründlich geplant werden. Wenn nicht benötigt, MUSS die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

SYS.1.2.3.A2 Sichere Installation von Windows Server (B)

Wenn vom Funktionsumfang her ausreichend, MUSS die Server-Core-Variante installiert werden. Andernfalls MUSS begründet werden, warum die Server-Core-Variante nicht genügt.

SYS.1.2.3.A3 Telemetrie- und Nutzungsdaten unter Windows Server (B)

Um die Übertragung von Diagnose- und Nutzungsdaten an Microsoft stark zu reduzieren, MUSS das Telemetrie-Level 0 (Security) auf dem Windows Server konfiguriert werden. Wenn diese Einstellung nicht wirksam umgesetzt wird, dann MUSS durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass die Daten nicht an den Hersteller übertragen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.2.3.A4 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)

Maßnahmen zum Schutz vor Exploits SOLLTEN für alle Programme und Dienste aktiviert werden, die den Exploit-Schutz von Windows (vgl. Verweis in Kapitel 4.1 *Wissenswertes*) unterstützen.

SYS.1.2.2.A5 Sichere Authentisierung und Autorisierung in Windows Server (S)

In Windows Server SOLLTEN alle Konten von Benutzenden Mitglied der Sicherheitsgruppe „Protected Users“ sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von „Protected Users“ sein. Dienste-Konten in Windows Server SOLLTEN Mitglied der Gruppe „Managed Service Account“ sein.

SYS.1.2.3.A6 Sicherheit beim Fernzugriff über RDP (S)

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der Berechtigten und IT-Systeme für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Berechtigungen festgelegt werden. Es SOLLTEN Mechanismen des Betriebssystems berücksichtigt werden, um die übertragenen Anmeldeinformationen zu schützen (z. B. *Remote Credential Guard* oder *RestrictedAdmin*). In komplexen Infrastrukturen SOLLTE das RDP-Zielsystem nur durch ein dazwischengeschaltetes RDP-Gateway erreicht werden können. Für die Verwendung von RDP SOLLTE eine Prüfung und deren Umsetzung sicherstellen, dass die nachfolgend aufgeführten Komfortfunktionen im Einklang mit dem Schutzbedarf des Zielsystems stehen:

- die Verwendung der Zwischenablage,
- die Einbindung von Wechselmedien und Netzlaufwerken sowie
- die Nutzung der Dateiablagen, von weiteren Geräten und Ressourcen, wie z. B. Smartcard-Lesegeräten.

Die eingesetzten kryptografischen Protokolle und Algorithmen SOLLTEN den internen Vorgaben der Institution entsprechen.

Sofern der Einsatz von Remote-Desktopzugriffen nicht vorgesehen ist, SOLLTEN diese vollständig deaktiviert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.2.3.A7 Verwendung der Windows PowerShell (H)

Die PowerShell-Ausführung SOLLTE zentral protokolliert werden. Die erzeugten Protokolle SOLLTEN geeignet überwacht werden. Die Ausführung von PowerShell-Skripten SOLLTE mit dem Befehl *Set-ExecutionPolicy AllSigned* eingeschränkt werden, um zu verhindern, dass unsignierte Skripte (versehentlich) ausgeführt werden. Ältere Windows PowerShell-Versionen SOLLTEN deaktiviert werden. Der Einsatz des PowerShell Constrained Language Mode SOLLTE geprüft werden. Zur Einschränkung der Windows PowerShell SOLLTE bei Windows Server mithilfe von Just Enough Administration (JEA) eine rollenbasierte Administration implementiert werden.

SYS.1.2.3.A8 Nutzung des Virtual Secure Mode (VSM) (H)

Bei der Nutzung des Virtual Secure Mode (VSM) SOLLTE berücksichtigt werden, dass forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt oder erschwert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Der Hersteller Microsoft stellt unter anderem folgende weiterführende Informationen zu Windows Server bereit:

- Windows Server – Dokumentation
  https://docs.microsoft.com/en-us/windows-server/
- Neuerungen in Windows Server 2019:
  https://docs.microsoft.com/en-us/windows-server/get-started-19/whats-new-19
- Neuerungen in Windows Server 2022:
  https://docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022
- Vergleich der Standard- und Datacenter-Editionen von Windows Server 2019:
  https://docs.microsoft.com/en-us/windows-server/get-started-19/editions-comparison-19
- Vergleich der Standard- und Datacenter-Editionen von Windows Server 2022:
  https://docs.microsoft.com/en-us/windows-server/get-started/editions-comparison-windows-server-2022
- Fixed Lifecycle-Richtlinie
  https://support.microsoft.com/en-us/help/14085/fixed-lifecycle-policy
- Entfernte oder zur Ersetzung vorgesehene Features in Windows Server 2019:
  https://docs.microsoft.com/en-us/windows-server/get-started-19/removed-features-19
- Security and Assurance (Übersicht):
  https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance
- Microsoft Security Compliance Toolkit 1.0:
  https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10
- Anpassen des Exploit-Schutzes
  https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection
- Schutz und Verwaltung von Anmeldeinformationen
  https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/credentials-protection-and-management
- Schützen von Remote Desktop Anmeldeinformationen mit Windows Defender Remote Credential Guard
  https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard

- Konfigurieren von Windows-Diagnosedaten in Ihrer Organisation
  https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization
- Liste von Sicherheitsereignissen unter Windows Server:
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
- Windows Server Guidance to protect against Speculative Execution:
  https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-speculative-execution
- Übersicht zur Windows-Authentifizierung
  https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security", insbesondere in Area SY1.2 Server Configuration, Vorgaben für den Einsatz von Servern.

Das National Institute of Standards and Technology (NIST) stellt das Dokument ,,Guide to General Server Security: NIST Special Publication 800-123", Juli 2008 zur Verfügung.

Das BSI stellt im Rahmen der Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10 (SiSyPHuS Win10), Empfehlungen zur sicheren Konfiguration und Deaktivierung von Telemetrie zur Verfügung, die auch auf Windows Server zutreffen:
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.3 Server unter Linux und Unix

1. Beschreibung

1.1. Einleitung

Auf Server-Systemen werden häufig die Betriebssysteme Linux oder Unix eingesetzt. Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux bezeichnet hingegen kein klassisches Unix, sondern ist ein funktionelles Unix-System. Das heißt, dass der Linux-Kernel nicht auf dem ursprünglichen Quelltext basiert, aus dem sich die verschiedenen Unix-Derivate entwickelt haben. In diesem Baustein werden alle Betriebssysteme der Unix-Familie betrachtet, also auch Linux als funktionelles Unix-System. Da sich die Konfiguration und der Betrieb von Linux- und Unix-Servern ähneln, werden in diesem Baustein Linux und Unix sprachlich als „Unix-Server" bzw. „unixartig" zusammengefasst.

Linux ist freie Software, die von der Open-Source-Gemeinschaft entwickelt wird. Das bedeutet, dass sie von jedem genutzt, kopiert, verteilt und verändert werden darf. Daneben gibt es Unternehmen, die die verschiedenen Software-Komponenten zu einer Distribution zusammenfassen und pflegen sowie weitere Dienstleistungen anbieten. Für Linux-Server werden häufig die Distributionen Debian, Red Hat Enterprise Linux / CentOS, SUSE Linux Enterprise / openSUSE oder Ubuntu Server eingesetzt. Darüber hinaus gibt es für spezielle Einsatzzwecke und Geräte zugeschnittene Linux-Distributionen wie OpenWRT für Router.

Die auf einem Unix-Server angebotenen Dienste sind oft zentral und daher in besonderem Maße exponiert. Aus diesem Grund sind Unix-Server nicht nur für Geschäftsprozesse oder Fachaufgaben kritisch, sondern geraten außerdem häufig in den Fokus von Angriffen. Deswegen kommt der Verfügbarkeit und Absicherung von Unix-Servern eine besondere Bedeutung zu.

1.2. Zielsetzung

Ziel des Bausteins ist der Schutz von Informationen, die von Unix-Servern bereitgestellt und verarbeitet werden. Die Anforderungen des Bausteins gelten vorrangig für Linux-Server, können aber generell für Unix-Server adaptiert werden. Es werden Anforderungen formuliert, wie das Betriebssystem unabhängig vom Einsatzzweck des Servers konfiguriert und betrieben werden soll.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.3 *Server unter Linux und Unix* ist für alle Server anzuwenden, auf denen Linux- oder Unix-basierte Betriebssysteme eingesetzt werden.

Der Baustein enthält grundsätzliche Anforderungen zur Einrichtung und zum Betrieb von Unix-Servern. Er konkretisiert und ergänzt die Aspekte, die im Baustein SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Unix-Systemen. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

Sicherheitsanforderungen möglicher Server-Funktionen wie Webserver (siehe APP.3.2 *Webserver*) oder E-Mail-Server (siehe APP.5.3 *Allgemeiner E-Mail-Client und -Server*) werden nicht in dem vorliegenden Baustein betrachtet, sondern sind Gegenstand eigener Bausteine. Eine Ausnahme ist der Unix-spezifische Server-Dienst SSH, der ebenfalls in diesem Baustein behandelt wird. Das Thema Virtualisierung wird ebenfalls nicht im vorliegenden Baustein beleuchtet, sondern im Baustein SYS.1.5 *Virtualisierung*.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.3 *Server unter Linux und Unix* von besonderer Bedeutung.

2.1. Ausspähen von Informationen über das System und über Benutzende

Mit Hilfe verschiedener Unix-Programme ist es möglich, Daten abzufragen, die das IT-System über die Benutzenden speichert. Hiervon sind auch solche Daten betroffen, die Auskunft über das Leistungsprofil von Benutzenden geben können. Zu diesen Informationen zählen sowohl Informationen über weitere angemeldete Benutzende wie auch technische Informationen zur Betriebssysteminstallation und -konfiguration.

Beispielsweise kann mit einem einfachen Programm, das in einem bestimmten Zeitintervall die Informationen auswertet, die der Befehl „who" liefert, jeder Benutzende ein genaues Nutzungsprofil für einen Account erstellen. So lassen sich auf diese Weise die Abwesenheitszeiten von Systemadministrierenden feststellen, um diese Zeiten für unberechtigte Handlungen zu nutzen. Des Weiteren lässt sich feststellen, welche Terminals für einen privilegierten Zugang zugelassen sind. Weitere Programme mit ähnlichen Möglichkeiten zum Datenmissbrauch sind „finger" oder „ruser".

2.2. Ausnutzbarkeit der Skriptumgebung

In Unix-Betriebssystemen werden oft Skriptsprachen genutzt. Skripte sind eine Auflistung von einzelnen Kommandos, die in einer Textdatei gespeichert und beispielsweise in der Kommandozeile aufgerufen werden. Durch den großen Funktionsumfang der Skriptumgebung können Angreifende Skripte umfangreich für ihre Zwecke missbrauchen. Darüber hinaus können aktivierte Skriptsprachen nur sehr schwer eingedämmt werden.

2.3. Dynamisches Laden von gemeinsam genutzten Bibliotheken

Mit der Kommandozeilenoption LD_PRELOAD wird eine dynamische Bibliothek vor allen anderen Standardbibliotheken, die in einer Anwendung benötigt werden, geladen. Dadurch lassen sich gezielt einzelne Funktionen der Standardbibliotheken durch eigene überschreiben. Angreifende könnten das Betriebssystem beispielsweise so manipulieren, dass Schadfunktionen bei der Nutzung von bestimmten Anwendungen mit ausgeführt werden.

2.4. Software aus Drittquellen

Bei unixartigen IT-Systemen kommt es vor, dass Benutzende Softwarequellcode selbst herunterladen und kompilieren, statt fertige Softwarepakete zu installieren. Wenn fertige Softwarepakete genutzt werden, werden diese außerdem in einigen Fällen aus Drittquellen ohne weitere Prüfung installiert, statt ausschließlich aus den vorhandenen Paketquellen des herstellenden Unternehmens. Jeder dieser alternativen Wege der Softwareinstallation birgt zusätzliche Risiken, da dadurch fehlerhafte oder inkompatible Software sowie Schadsoftware installiert werden kann.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.3 *Server unter Linux und Unix* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle

hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.3.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.3.A2 Sorgfältige Vergabe von IDs (B)

Jeder Login-Name, jede User-ID (UID) und jede Gruppen-ID (GID) DARF NUR einmal vorkommen. Jedes Konto von Benutzenden MUSS Mitglied mindestens einer Gruppe sein. Jede in der Datei */etc/passwd* vorkommende GID MUSS in der Datei */etc/group* definiert sein. Jede Gruppe SOLLTE nur die Konten enthalten, die unbedingt notwendig sind. Bei vernetzten Systemen MUSS außerdem darauf geachtet werden, dass die Vergabe von Benutzenden- und Gruppennamen, UID und GID im Systemverbund konsistent erfolgt, wenn beim systemübergreifenden Zugriff die Möglichkeit besteht, dass gleiche UIDs bzw. GIDs auf den Systemen unterschiedlichen Benutzenden- bzw. Gruppennamen zugeordnet werden könnten.

SYS.1.3.A3 Kein automatisches Einbinden von Wechsellaufwerken (B)

Wechseldatenträger wie z. B. USB-Sticks oder CDs/DVDs DÜRFEN NICHT automatisch eingebunden werden.

SYS.1.3.A4 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (B)

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, MUSS ASLR und DEP/NX im Kernel aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken, wie z. B. Heap- und Stackschutz, DÜRFEN NICHT deaktiviert werden.

SYS.1.3.A5 Sichere Installation von Software-Paketen (B)

Wenn zu installierende Software aus dem Quellcode kompiliert werden soll, DARF diese NUR unter einem unprivilegierten Konto entpackt, konfiguriert und übersetzt werden. Anschließend DARF die zu installierende Software NICHT unkontrolliert in das Wurzeldateisystem des Betriebssystems installiert werden.

Wird die Software aus dem Quelltext übersetzt, SOLLTEN die gewählten Parameter geeignet dokumentiert werden. Anhand dieser Dokumentation SOLLTE die Software jederzeit nachvollziehbar und reproduzierbar kompiliert werden können. Alle weiteren Installationsschritte SOLLTEN dabei ebenfalls dokumentiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.3.A6 Verwaltung von Benutzenden und Gruppen (S)

Zur Verwaltung von Benutzenden und Gruppen SOLLTEN die entsprechenden Verwaltungswerkzeuge genutzt werden. Von einer direkten Bearbeitung der Konfigurationsdateien */etc/passwd, /etc/shadow*, */etc/group* und */etc/sudoers* SOLLTE abgesehen werden.

SYS.1.3.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.3.A8 Verschlüsselter Zugriff über Secure Shell (S)

Um eine verschlüsselte und authentisierte, interaktive Verbindung zwischen zwei IT-Systemen aufzubauen, SOLLTE ausschließlich Secure Shell (SSH) verwendet werden. Alle anderen Protokolle, deren Funktionalität durch Secure Shell abgedeckt wird, SOLLTEN vollständig abgeschaltet werden. Für die Authentifizierung SOLLTEN vorrangig Zertifikate anstatt eines Passworts verwendet werden.

SYS.1.3.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.3.A10 Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (S)

Dienste und Anwendungen SOLLTEN mit einer individuellen Sicherheitsarchitektur geschützt werden (z. B. mit AppArmor oder SELinux). Auch chroot-Umgebungen sowie LXC- oder Docker-Container SOLLTEN dabei berücksichtigt werden. Es SOLLTE sichergestellt sein, dass mitgelieferte Standardprofile bzw. -regeln aktiviert sind.

SYS.1.3.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.3.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.3.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.3.A14 Verhinderung des Ausspähens von Informationen über das System und über Benutzende (H)

Die Ausgabe von Informationen über das Betriebssystem und der Zugriff auf Protokoll- und Konfigurationsdateien SOLLTE für Benutzende auf das notwendige Maß beschränkt werden. Außerdem SOLLTEN bei Befehlsaufrufen keine vertraulichen Informationen als Parameter übergeben werden.

SYS.1.3.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.3.A16 Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (H)

Die Nutzung von Systemaufrufen SOLLTE insbesondere für exponierte Dienste und Anwendungen auf die unbedingt notwendige Anzahl beschränkt werden. Die Standardprofile bzw. -regeln von z. B. SELinux, AppArmor SOLLTEN manuell überprüft und unter Umständen an die eigenen Sicherheitsrichtlinien angepasst werden. Falls erforderlich, SOLLTEN neue Regeln bzw. Profile erstellt werden.

SYS.1.3.A17 Zusätzlicher Schutz des Kernels (H)

Es SOLLTEN speziell gehärtete Kernels (z. B. grsecurity, PaX) und geeignete Schutzmaßnahmen wie Speicherschutz oder Dateisystemabsicherung umgesetzt werden, die eine Ausnutzung von Schwachstellen und die Ausbreitung im Betriebssystem verhindern.

4. Weiterführende Informationen

4.1. Wissenswertes

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Guide to General Server Security: NIST Special Publication 800-123“, Juli 2008 zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.5 Virtualisierung

1. Beschreibung

1.1. Einleitung

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen IT-System ausgeführt. Ein solches physisches IT-System wird als „Virtualisierungsserver" bezeichnet. Mehrere Virtualisierungsserver können zu einer virtuellen Infrastruktur zusammengefasst werden. Darin können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Die Virtualisierung von IT-Systemen bietet viele Vorteile für den IT-Betrieb in einem Informationsverbund. So können beispielsweise Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der physischen IT-Systeme effizienter genutzt werden. Allerdings ist die Virtualisierung auch eine Herausforderung für den Betrieb des Informationsverbunds. Da durch die eingesetzte Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund berührt werden, müssen Wissen und Erfahrungen aus diesen Bereichen zusammengeführt werden. Zudem können sich Probleme auf einem Virtualisierungsserver auch auf alle anderen virtuellen IT-Systeme, die auf demselben Virtualisierungsserver betrieben werden, auswirken. Ebenso können sich virtuelle IT-Systeme gegenseitig in ihrem Betrieb stören.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es aufzuzeigen, wie Virtualisierungsserver im Informationsverbund sicher eingeführt und betrieben werden können.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.5 *Virtualisierung* ist auf jeden Virtualisierungsserver anzuwenden.

Neben dem vorliegenden Baustein müssen auch die jeweils relevanten Server- oder Client-Bausteine der Schicht SYS *IT-Systeme* auf jeden Virtualisierungsserver angewandt werden. Neben den betriebssystemspezifischen Bausteinen müssen außerdem die Bausteine SYS.1.1 *Allgemeiner Server* bzw. SYS.2.1 *Allgemeiner Client* angewendet werden, da in diesen Bausteinen die plattformunabhängigen Sicherheitsaspekte für Server bzw. Clients zusammengefasst sind.

In diesem Baustein wird nur die Virtualisierung vollständiger IT-Systeme behandelt. Andere Techniken, die teilweise ebenfalls mit dem Wort „Virtualisierung" in Verbindung gebracht werden (z. B. Anwendungsvirtualisierung mittels Terminalservern, Storage-Virtualisierung und Container), sind nicht Gegenstand dieses Bausteins.

Im Bereich der Software-Entwicklung werden die Begriffe *„Virtuelle Maschine"* und *„Virtueller-Maschinen-Monitor"* auch für Laufzeitumgebungen benutzt, z. B. wenn Java oder Microsoft .NET eingesetzt werden. Solche Laufzeitumgebungen werden in diesem Baustein ebenfalls nicht betrachtet.

Virtuelle Infrastrukturen werden in der Regel mit speziellen Managementsystemen verwaltet. Da mit diesen IT-Systemen umfassend auf die Virtualisierungsinfrastruktur zugegriffen werden kann, ist es wichtig, diese ausreichend abzusichern. Das betrifft sowohl den physischen oder virtuellen Server, auf dem die Management-Software ausgeführt wird, als auch das Produkt selber.

Virtualisierungsumgebungen werden meistens gemeinsam mit Speichernetzen (NAS oder SAN) eingesetzt. Die Anbindung und Absicherung dieser Systeme werden in diesem Baustein ebenfalls nicht betrachtet (siehe hierfür Baustein SYS.1.8 *Speicherlösungen*).

Durch die Virtualisierung müssen die Netze der Institution anders strukturiert werden. Dieses Thema wird in diesem Baustein nicht umfassend behandelt. Dafür müssen die Anforderungen des Bausteins NET.1.1 *Netzarchitektur und -design* erfüllt werden. Auch die Netzvirtualisierung wird im vorliegenden Baustein nicht in der notwendigen Tiefe beleuchtet.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.5 *Virtualisierung* von besonderer Bedeutung.

2.1. Fehlerhafte Planung der Virtualisierung

Ein Virtualisierungsserver ermöglicht den Betrieb virtueller IT-Systeme, integriert die IT-Systeme in das Rechenzentrum und steuert dabei deren Anbindung an weitere Infrastrukturelemente, z. B. Netze (inklusive Speichernetze). Wird nicht geplant, wie die Virtualisierungsserver technisch und organisatorisch in die bestehende Infrastruktur zu integrieren sind, kann dies dazu führen, dass die Zuständigkeiten für unterschiedliche Bereiche womöglich nicht klar definiert sind, z. B. für Anwendungen, Betriebssysteme und Netzkomponenten. Weiterhin können sich die Zuständigkeiten verschiedener Bereiche überschneiden oder es ist keine passende Rechtestruktur vorhanden, um administrative Zugriffe für die unterschiedlichen Bereiche zu trennen.

2.2. Fehlerhafte Konfiguration der Virtualisierung

Durch Virtualisierung ändert sich die Art und Weise, wie Server provisioniert werden. Ressourcen wie CPU, RAM, Netzanbindung und Speicher werden in der Regel zentral über ein Managementsystem konfiguriert und sind nicht mehr durch Hardware und Verkabelung vorgegeben. Dadurch können schnell Fehler in der Konfiguration entstehen. Wird beispielsweise ein hoch schutzbedürftiges virtuelles IT-System fälschlicherweise in einer externen Demilitarisierten Zone (DMZ) platziert, ist es folglich aus dem Internet erreichbar und somit einem erhöhten Risiko ausgesetzt.

2.3. Unzureichende Ressourcen für virtuelle IT-Systeme

Virtualisierungsserver benötigen für den Betrieb der virtuellen IT-Systeme Speicherplatz, der entweder lokal im Virtualisierungsserver selbst oder in einem Speichernetz bereitgestellt wird. Werden die hierfür benötigten Speicherkapazitäten nicht ausreichend groß geplant, bestehen weitreichende Risiken für die Verfügbarkeit der virtuellen IT-Systeme und die Integrität der in ihnen verarbeiteten Informationen. Das gilt insbesondere dann, wenn spezielle Virtualisierungsfunktionen, wie Snapshots oder die Überbuchung von Speicherplatz, benutzt werden.

Engpässe können nicht nur den Speicherplatz auf Festplatten oder in Speichernetzen betreffen, sondern auch die Prozessorleistung, den Arbeitsspeicher (RAM), oder die Netzanbindung. Außerdem könnten sich durch unzureichende Ressourcen auf dem Virtualisierungsserver die virtuellen Maschinen gegenseitig in ihrem Betrieb stören und letztlich nicht mehr korrekt arbeiten oder ganz ausfallen.

2.4. Informationsabfluss oder Ressourcen-Engpass durch Snapshots

Durch einen Snapshot kann der Zustand einer virtuellen Maschine eingefroren und gesichert werden. Wird ein solcher Snapshot zu einem späteren Zeitpunkt wiederhergestellt, gehen alle in der Zwischenzeit vorgenommenen Änderungen verloren. Dadurch können auch bereits gepatchte Sicherheitslücken wieder offen sein. Weiterhin können durch offene Dateien, Dateitransfers oder Datenbanktransaktionen zum Zeitpunkt des Snapshots inkonsistente Daten entstehen.

Außerdem können Snapshots bei Angriffen dazu missbraucht werden, um unberechtigt auf die Daten eines virtuellen IT-Systems zuzugreifen. Denn wenn der Snapshot im laufenden Betrieb erstellt wurde, ist auch der Inhalt des Hauptspeichers auf der Festplatte gesichert worden und kann auf einer virtuellen Umgebung außerhalb der ursprünglichen IT-Infrastruktur wiederhergestellt und analysiert werden. Ebenso können Snapshots sehr groß werden und dadurch kann die verfügbare Speicherkapazität knapp werden.

2.5. Ausfall des Verwaltungsservers für Virtualisierungssysteme

Da über den Verwaltungsserver sämtliche Funktionen einer virtuellen Infrastruktur gesteuert und administriert werden, führt ein Ausfall dieses Verwaltungssystems dazu, dass keine Konfigurationsänderungen an der virtuellen Infrastruktur durchgeführt werden können. Der IT-Betrieb kann in dieser Zeit nicht auf auftretende Probleme wie Ressourcenengpässe oder den Ausfall einzelner Virtualisierungsserver reagieren und keine neuen Virtualisierungsserver in die Infrastruktur integrieren oder neue virtuelle IT-Systeme anlegen. Auch die Live-Migration und damit die dynamische Zuteilung von Ressourcen für einzelne Gast-Systeme ist ohne Verwaltungsserver nicht möglich.

2.6. Missbräuchliche Nutzung von Gastwerkzeugen

Gastwerkzeuge werden in den virtuellen Maschinen häufig mit sehr hohen Berechtigungen ausgeführt. Dadurch lassen sie sich beispielsweise für Denial-of-Service-Angriffe missbrauchen oder Angreifende übernehmen mit ihnen gleich den ganzen Virtualisierungsserver.

2.7. Kompromittierung der Virtualisierungssoftware

Die Virtualisierungssoftware (auch „Hypervisor“) ist die zentrale Komponente eines Virtualisierungsservers. Sie steuert alle auf diesem Server ausgeführten virtuellen Maschinen und teilt ihnen Prozessor- und Speicherressourcen zu. Wird diese Komponente erfolgreich angegriffen, führt dies auch dazu, dass alle virtuellen IT-Systeme, die auf dem Virtualisierungsserver ausgeführt werden, kompromittiert sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.5 *Virtualisierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.5.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.5.A2 Sicherer Einsatz virtueller IT-Systeme (B)

Jede Person, die virtuelle IT-Systeme administriert, MUSS wissen, wie sich eine Virtualisierung auf die betriebenen IT-Systeme und Anwendungen auswirkt. Die Zugriffsrechte für Administrierende auf virtuelle IT-Systeme MÜSSEN auf das tatsächlich notwendige Maß reduziert sein.

Es MUSS gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur verfügbar sind. Auch MUSS geprüft werden, ob die Anforderungen an die Isolation und Kapselung der virtuellen IT-Systeme sowie der darauf betriebenen Anwendungen hinreichend erfüllt sind. Weiterhin MÜSSEN die eingesetzten virtuellen IT-Systeme den Anforderungen an die Verfügbarkeit und den Datendurchsatz genügen. Im laufenden Betrieb MUSS die Performance der virtuellen IT-Systeme überwacht werden.

SYS.1.5.A3 Sichere Konfiguration virtueller IT-Systeme (B)

Gast-Systeme DÜRFEN NICHT auf Geräte und Schnittstellen des Virtualisierungsservers zugreifen. Ist eine solche Verbindung jedoch notwendig, MUSS diese exklusiv zugeteilt werden. Sie DARF NUR für die notwendige Dauer von den Administrierenden des Host-Systems hergestellt werden. Dafür MÜSSEN verbindliche Regelungen festgelegt werden.

Virtuelle IT-Systeme SOLLTEN nach den Sicherheitsrichtlinien der Institution konfiguriert und geschützt werden.

SYS.1.5.A4 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen (B)

Es MUSS sichergestellt werden, dass bestehende Sicherheitsmechanismen (z. B. Firewalls) und Monitoring-Systeme nicht über virtuelle Netze umgangen werden können. Auch MUSS ausgeschlossen sein, dass über virtuelle IT-Systeme, die mit mehreren Netzen verbunden sind, unerwünschte Netzverbindungen aufgebaut werden können.

Netzverbindungen zwischen virtuellen IT-Systemen und physischen IT-Systemen sowie für virtuelle Firewalls SOLLTEN gemäß den Sicherheitsrichtlinien der Institution konfiguriert werden.

SYS.1.5.A5 Schutz der Administrationsschnittstellen (B)

Alle Administrations- und Management-Zugänge zum Managementsystem und zu den Host-Systemen MÜSSEN eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Um die Virtualisierungsserver oder die Managementsysteme zu administrieren bzw. zu überwachen, SOLLTEN als sicher geltende Protokolle eingesetzt werden. Sollte dennoch auf unsichere Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz genutzt werden.

SYS.1.5.A6 Protokollierung in der virtuellen Infrastruktur (B)

Betriebszustand, Auslastung und Netzanbindungen der virtuellen Infrastruktur MÜSSEN laufend protokolliert werden. Werden Kapazitätsgrenzen erreicht, SOLLTEN virtuelle Maschinen verschoben werden. Zudem SOLLTE eventuell die Hardware erweitert werden. Auch MUSS überwacht werden, ob die virtuellen Netze den jeweiligen virtuellen IT-Systemen korrekt zugeordnet sind.

SYS.1.5.A7 Zeitsynchronisation in virtuellen IT-Systemen (B)

Die Systemzeit aller produktiv eingesetzten virtuellen IT-Systeme MUSS immer synchron sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.5.A8 Planung einer virtuellen Infrastruktur (S) [Planende]

Der Aufbau der virtuellen Infrastruktur SOLLTE detailliert geplant werden. Dabei SOLLTEN die geltenden Regelungen und Richtlinien für den Betrieb von IT-Systemen, Anwendungen und Netzen (inklusive Speichernetzen) berücksichtigt werden. Wenn mehrere virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden, SOLLTEN KEINE Konflikte hinsichtlich des Schutzbedarfs der IT-Systeme auftreten. Weiterhin SOLLTEN die Aufgaben der einzelnen Gruppen, die für die Administration zuständig sind, festgelegt und klar voneinander abgegrenzt werden. Es SOLLTE auch geregelt werden, wer für den Betrieb welcher Komponente verantwortlich ist.

SYS.1.5.A9 Netzplanung für virtuelle Infrastrukturen (S) [Planende]

Der Aufbau des Netzes für virtuelle Infrastrukturen SOLLTE detailliert geplant werden. Auch SOLLTE geprüft werden, ob für bestimmte Virtualisierungsfunktionen (wie z. B. die Live-Migration) ein eigenes Netz aufgebaut und genutzt werden muss. Es SOLLTE geplant werden, welche Netzsegmente aufgebaut werden müssen (z. B. Managementnetz, Speichernetz). Es SOLLTE festgelegt werden, wie die Netzsegmente sich sicher voneinander trennen und schützen lassen. Dabei SOLLTE sichergestellt werden, dass das produktive Netz vom Managementnetz getrennt ist (siehe SYS.1.5.A11 *Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz*). Auch die Verfügbarkeitsanforderungen an das Netz SOLLTEN erfüllt werden.

SYS.1.5.A10 Einführung von Verwaltungsprozessen für virtuelle IT-Systeme (S)

Für Virtualisierungsserver und virtuelle IT-Systeme SOLLTEN Prozesse für die Inbetriebnahme, die Inventarisierung, den Betrieb und die Außerbetriebnahme definiert und etabliert werden. Die Prozesse SOLLTEN dokumentiert und regelmäßig aktualisiert werden.

Wenn der Einsatz von virtuellen IT-Systemen geplant wird, SOLLTE festgelegt werden, welche Virtualisierungsfunktionen die virtuellen IT-Systeme benutzen dürfen. Test- und Entwicklungsumgebungen SOLLTEN NICHT auf demselben Virtualisierungsserver betrieben werden wie produktive virtuelle IT-Systeme.

SYS.1.5.A11 Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz (S)

Die Virtualisierungsinfrastruktur SOLLTE ausschließlich über ein separates Managementnetz administriert werden (siehe NET.1.1 *Netzarchitektur und -design*). Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert werden. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden (siehe NET.1.2 *Netzmanagement*).

SYS.1.5.A12 Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur (S)

Anhand der in der Planung definierten Aufgaben und Rollen (siehe SYS.1.5.A8 *Planung einer virtuellen Infrastruktur*) SOLLTE für die Administration der virtuellen IT-Systeme und Netze sowie der Virtualisierungsserver und der Managementumgebung ein Rechte- und Rollenkonzept erstellt und umgesetzt werden. Alle Komponenten der virtuellen Infrastruktur SOLLTEN in ein zentrales Identitäts- und Berechtigungsmanagement eingebunden werden. Administrierende von virtuellen Maschinen und Administrierende der Virtualisierungsumgebung SOLLTEN unterschieden werden. Sie SOLLTEN mit unterschiedlichen Zugriffsrechten ausgestattet werden.

Weiterhin SOLLTE die Managementumgebung virtuelle Maschinen zur geeigneten Strukturierung gruppieren können. Die Rollen der Administrierenden SOLLTEN entsprechend zugeteilt werden.

SYS.1.5.A13 Auswahl geeigneter Hardware für Virtualisierungsumgebungen (S)

Die verwendete Hardware SOLLTE kompatibel mit der eingesetzten Virtualisierungslösung sein. Dabei SOLLTE darauf geachtet werden, dass das herstellende Unternehmen der Virtualisierungslösung über den geplanten Einsatzzeitraum auch Support für die betriebene Hardware anbietet.

SYS.1.5.A14 Einheitliche Konfigurationsstandards für virtuelle IT-Systeme (S)

Für die eingesetzten virtuellen IT-Systeme SOLLTEN einheitliche Konfigurationsstandards definiert werden. Die virtuellen IT-Systeme SOLLTEN nach diesen Standards konfiguriert werden. Die Konfigurationsstandards SOLLTEN regelmäßig überprüft werden. Sie SOLLTEN, falls erforderlich, angepasst werden.

SYS.1.5.A15 Betrieb von Gast-Betriebssystemen mit unterschiedlichem Schutzbedarf (S)

Falls virtuelle IT-Systeme mit unterschiedlichem Schutzbedarf gemeinsam auf einem Virtualisierungsserver betrieben werden, SOLLTE dabei sichergestellt sein, dass die virtuellen IT-Systeme ausreichend gekapselt und voneinander isoliert sind. Auch SOLLTE dann die Netztrennung in der eingesetzten Virtualisierungslösung ausreichend sicher sein. Ist das nicht der Fall, SOLLTEN weitergehende Sicherheitsmaßnahmen identifiziert und umgesetzt werden.

SYS.1.5.A16 Kapselung der virtuellen Maschinen (S)

Die Funktionen „Kopieren“ und „Einfügen“ von Informationen zwischen virtuellen Maschinen SOLLTEN deaktiviert sein.

SYS.1.5.A17 Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur (S)

Der Betriebszustand der virtuellen Infrastruktur SOLLTE überwacht werden. Dabei SOLLTE unter anderem geprüft werden, ob noch ausreichend Ressourcen verfügbar sind. Es SOLLTE auch geprüft werden, ob es eventuell Konflikte bei gemeinsam genutzten Ressourcen eines Virtualisierungsservers gibt.

Weiterhin SOLLTEN die Konfigurationsdateien der virtuellen IT-Systeme regelmäßig auf unautorisierte Änderungen überprüft werden.

Wird die Konfiguration der Virtualisierungsinfrastruktur geändert, SOLLTEN die Änderungen geprüft und getestet werden, bevor sie umgesetzt werden.

SYS.1.5.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.5.A19 Regelmäßige Audits der Virtualisierungsinfrastruktur (S)

Es SOLLTE regelmäßig auditiert werden, ob der Ist-Zustand der virtuellen Infrastruktur dem in der Planung festgelegten Zustand entspricht. Auch SOLLTE regelmäßig auditiert werden, ob die Konfiguration der virtuellen Komponenten die vorgegebene Standardkonfiguration einhält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.5.A20 Verwendung von hochverfügbaren Architekturen (H) [Planende]

Die virtuelle Infrastruktur SOLLTE hochverfügbar ausgelegt werden. Alle Virtualisierungsserver SOLLTEN in Clustern zusammengeschlossen werden.

SYS.1.5.A21 Sichere Konfiguration virtueller IT-Systeme bei erhöhtem Schutzbedarf (H)

Für virtuelle IT-Systeme SOLLTEN Überbuchungsfunktionen für Ressourcen deaktiviert werden.

SYS.1.5.A22 Härtung des Virtualisierungsservers (H)

Der Virtualisierungsserver SOLLTE gehärtet werden. Um virtuelle IT-Systeme voreinander und gegenüber dem Virtualisierungsserver zusätzlich zu isolieren und zu kapseln, SOLLTEN Mandatory Access Controls (MACs) eingesetzt werden. Ebenso SOLLTE das IT-System, auf dem die Management-Software installiert ist, gehärtet werden.

SYS.1.5.A23 Rechte-Einschränkung der virtuellen Maschinen (H)

Alle Schnittstellen und Kommunikationskanäle, die es einem virtuellen IT-System erlauben, Informationen über das Host-System auszulesen und abzufragen, SOLLTEN deaktiviert sein oder unterbunden werden. Weiterhin SOLLTE ausschließlich der Virtualisierungsserver auf seine Ressourcen zugreifen können. Virtuelle IT-Systeme SOLLTEN NICHT die sogenannten Pages des Arbeitsspeichers teilen.

SYS.1.5.A24 Deaktivierung von Snapshots virtueller IT-Systeme (H)

Für alle virtuellen IT-Systeme SOLLTE die Snapshot-Funktion deaktiviert werden.

SYS.1.5.A25 Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme (H)

Direkte Zugriffe auf die emulierten Konsolen virtueller IT-Systeme SOLLTEN auf ein Mindestmaß reduziert werden. Die virtuellen IT-Systeme SOLLTEN möglichst über das Netz gesteuert werden.

SYS.1.5.A26 Einsatz einer PKI (H) [Planende]

Für die mit Zertifikaten geschützte Kommunikation zwischen den Komponenten der IT-Infrastruktur SOLLTE eine Public-Key-Infrastruktur (PKI) eingesetzt werden.

SYS.1.5.A27 Einsatz zertifizierter Virtualisierungssoftware (H)

Es SOLLTE zertifizierte Virtualisierungssoftware der Stufe EAL 4 oder höher eingesetzt werden.

SYS.1.5.A28 Verschlüsselung von virtuellen IT-Systemen (H)

Alle virtuellen IT-Systeme SOLLTEN verschlüsselt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI gibt in seiner Veröffentlichung zur Cyber-Sicherheit BSI-CS 113: „Server-Virtualisierung" Empfehlungen zum Einsatz von Virtualisierung.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security" im Kapitel SYS.1.3 – Virtual Servers – Vorgaben für den Betrieb von virtuellen Servern.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-125 „Guide to Security for Full Virtualization Technologie" Empfehlungen zum Einsatz von Virtualisierung.